

REVIEW OF EDP CONTINGENCY PLANS

The Preliminary Survey Audit Program requires the audit staff to evaluate the auditee's EDP Contingency Plan as submitted to the Information Technology Department. This procedure provides guidelines in evaluating the completeness of the contingency plan.

EDP Contingency Plans refer to those procedures which provide for a controlled response to emergency situations and allow the computer system users to recover from interruptions in service with a minimum disruption in operations.

In order to be considered complete, an EDP Contingency Plan should address the following control objectives:

1. **Identification and Prioritization of Data Processing Resources.** The plan should identify those critical data processing application programs, operating systems, and data files that are critical to the department's mission and provide for priorities in the reestablishment of the processing of specific critical or sensitive application programs after a disaster occurs.
2. **Routine Backup Procedures and Offsite Storage of Backup Files.** The plan should provide data file backup procedures – including the regular copying of disk file content to tape or other magnetic media – to be performed routinely. The plan should also provide that backup files are regularly moved to off-site storage.
3. **Backup Site and Hardware.** The plan should provide for the backup site and backup computer hardware required for restoring the department's data processing operations after a disaster occurs.
4. **Programming for Backup Operations.** The plan should provide for adequate programming staff to operate the department's backup data processing operations.
5. **Telecommunications Services Restoration.** The plan should include procedures for reestablishing the telecommunications services used by the organization.
6. **Data File Recovery Procedures.** The plan should ensure that, in the event of a service interruption, there should be resources available to the facility to enable it to continue to operate. The plan should address such questions as: whether backup power supply will be invoked; whether a move to the backup facility will occur; whether backup files will be retrieved from off-site storage. The plan should also provide for the completion of critical jobs, following an interruption or loss of the computer configuration required to successfully complete the processing of such critical jobs.
7. **Disaster Recovery Supplies.** The plan should provide for more than one source of supplies – including stocks of any needed special forms – to be used in restoring the department's data processing operations after a disaster occurs.
8. **Personnel Safety and Training.** The plan should include emergency procedures to ensure the safety of its staff members and they should receive periodic training in the use of these procedures.
9. **Documentation and Testing.** The plan should be documented and tested on a regular basis to ensure that it remains current and operational.